**RISK IDENTIFICATION REPORT**

1. **Carry out a risk assessment of the Pampered Pets business as it stands currently (Knowledge and Understanding weighted at 25%). This should include:**
   1. **A selection of a risk assessment methodology with justifications for the selection.**

The company as it stands relates to more conventional/traditional risk assessment methodolgies compared to the NIST framework, which I've chosen for the second part, that focuses on managing contemporary digitalized business operations. The brick-and mortar company still uses old networked computers, with main revenue coming from face-to-face retail, hence, traditional risk assessment methodologies appear to be more appropriate for this example (Joh Partners, n.d.).

* 1. **A risk and threat modelling exercise that enumerates and evaluates the current threats and risks to the business.**

1. **Threat**: Online retail competitors **Risk:** Losing customers
2. **Threat**: Property rent cost **Risk:** Forced to relocate with additional costs related to workforce management, losing loyal customers, finding new supply chains
3. **Threat**: Cost of goods **Risk:** Increased expenditures on local suppliers
4. **Threat**: Cost of labour **Risk:** struggling to find new employees in suburb of Hashington-on-the-Water (Myers, 2019)
5. **Threat**: Outdated computer software used by Harry and the front desk department **Risk:** Increased risk of surface attack
6. **Threat**: Unsecured POS systems **Risk:** Compromised payment card including sensitive data (ColorTokens, 2024)
   1. **A list of potential mitigations to the identified risks and threats.**

* Digitalize operations and prioritize web-based sale
* Tracking rental costs and act accordingly
* Considering lower-cost suppliers without compromising quality
* Using verified computer software and POS systems

1. **Carry out a risk assessment around the potential digitalisation process as applied to the Pampered Pets business (Application and Understanding weighted at 15%, Criticality weighted at 15%). This should include:**
   1. **A selection of a risk assessment methodology with justifications for the selection.**

For the digitalization part of the risk identification report, I've decided to follow the guidlines provided by the National Institute of Standards and Technology (NIST). I've chosen this approach because it provides straightforward guidelines and measures to benchmark security standars against best practices, as opposed to the more certification-focused ISO standards, which may be unnecessary given the company's size (Kurri & Opirskyy, 2022).

* 1. **A list of proposed changes that form the basis of the digitalisation process/ transformation (e.g., e-commerce portal, ERP system, online marketing, blogs, etc. – note you do not have to include ALL these features).**

To achieve digital transformation, the company should implement:

* B2C online retail platform to reach larger number of customers.
* Warehouse management system to track inventory changes. (ERP as an automation system to track various processes (including human resources) shouldn't be needed for that size of the company).
* Online marketing (Considering pet food marketing on various social platforms)
* Customer relationship management system
* Analytical software & reporting (PowerBI) (Symonds, 2023)
  1. **A risk and threat modelling exercise that enumerates and evaluates the potential threats and risks to the business of the proposed changes.**

According to NIST methodology with the focus on STRIDE threat modeling, we can identify following threats and risks related to the company:

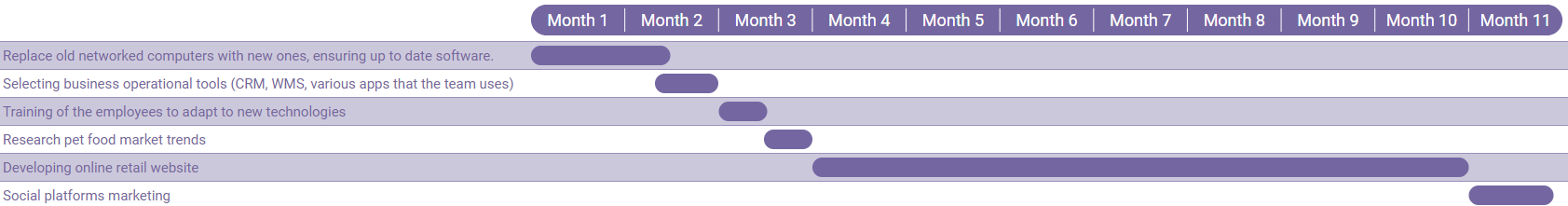
| **STRIDE RISK** | **Identified Threats** |
| --- | --- |
| **S**poofing | **Threat 1:** Accessing users accounts through impersonation.  **Threat 2:** Phishing attack. |
| **T**ampering | **Threat 1 :** Modifying inventory/sensitive customer data  **Threat 2 :** Parameter tampering attack  **Threat 3 :** Modifying value in a report to present false information |
| **R**epudiation | **Threat 1:** Adversary freely forges malicios activities without being spotted or recognised |
| **I**nformation Disclosure | **Threat 1:** Sensitive user's and company's data leakage |
| **D**enial of Service | **Threat 1:** Compromised webpage availability  **Threat 2:** Revenue loss and reputational damage (Sansone, n.d) |
| **E**levation of Privilege | **Threat 1:** Gaining access of an account (human or machine)  **Threat 2:** Execute malicious code and exploit software flaws (Haber, 2023) |

* 1. **A list of potential mitigations to the identified risks and threats.**

| **STRIDE RISK** | **Identified mitigation** |
| --- | --- |
| **S**poofing | **Mitigation 1:** Using Multi-Factor Authentication.  **Mitigation 2:** Educating employees. |
| **T**ampering | **Mitigation 1 :** Encrypting and backing up the data  **Mitigation 2 :**  Avoid including parameters into query string, using regex, server-side validation, validating inputs, use whitelist, session encryption  **Mitigation 3 :**  Appropriate authentication and authorisation, role based access |
| **R**epudiation | **Mitigation 1:** System monitoring |
| **I**nformation Disclosure | **Mitigation 1:** Data encryption. Store sensitive data separately |
| **D**enial of Service | **Mitigation 1:** Web application firewall, rate limiting, traffic routing  **Mitigation 2**: Building brand integrity |
| **E**levation of Privilege | **Mitigation 1:** Using proper authorization and authentication with role based access  **Mitigation 2:** Keeping software packages up-to-date |

1. **Finally, provide a summary of your recommendations for the business. Do you recommend that the digitalisation process be carried out? If so, what would be involved? What approach and timeline would you suggest? (Application and Understanding weighted at 10%, Criticality weighted at 10%)**

Digitalization should be the priority in order to increase business growth. The initial assumption of increasing the business growth by 50% can be achieved, given that at the moment company operates localy in small suburb. However, including international supply chain could reduce costs, yet the quality might be compromised due to prolonged transportation. Furthermore, the business shouldn't lose existing customers if the company doesn't provide online features because of the brand trusthworthiness perceived by local customers.



Gantt chart depicting the timeline of actions to be considered for the company's digital transformation

**References:**

* ColorTokens (2024) How Brick-And-Mortar Retailers Can Avoid Cyberattacks. Available from: <https://colortokens.com/blog/cybersecurity-for-brick-and-mortar-retailers/> [Accessed 27 June 2024]
* Haber, M. J. (2023) Privilege Escalation Attack & Defense Explained. BeyondTrust. Available from: <https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained> [Accessed 29 June 2024]
* Joh Partners (n.d) Understanding Traditional Risk Management Basics. Available from: <https://johpartners.com/understanding-traditional-risk-management-basics/> [Accessed 26 June 2024]
* Kurii, Y. & Opirskyy, I. (2022) Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013. CEUR Workshop Proceedings. Available from: <https://ceur-ws.org/Vol-3288/paper3.pdf> [Accessed 26 June 2024]
* Myers, A. (2019) 4 Challenges Facing Bricks-and-Mortars Retailers. WorkJam. Available from: <https://www.workjam.com/digital-workplace-blog/4-challenges-facing-brick-and-mortar-retailers/> [Accessed 27 June 2024]
* Sansone, I. (n.d.) The Damaging Impacts of DDoS Attacks. Corero. Available from: <https://www.corero.com/the-damaging-impacts-of-ddos-attacks/> [Accessed 29 June 2024]
* Symonds, C. (2023) Guide to digitalization: 10 ways to digitize your business. Factorial. Available from: <https://factorialhr.com/blog/digitalization/> [Accessed 28 June 2024]